#2

Form PTO 1449	ATTY. DOCKET NUMBER	L NUMBER 09/9356 54
U.S. Department of Commerce Patent and Trademark Office	NITT.0028	To Be Assigned
	APPLICANT KAMINAGA et al	
Information Disclosure Statement by Applicant	FILING DATE Concurrently Herewith	GROUP 2124

JC896 U.S. PTO 09/935654 08/24/01

U.S. Patent Documents

Examiner Initial		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBC LASS	FILING DATE

Foreign Patent Documents

Examiner Initial		DOCUMENT NUMBER	FILING DATE	COUNTRY	CLAS S	SUB-CLASS	TRANSLATION YES	TRANSLATION NO

Other Documents (Including Author, Title, Date Pertinent Pages, Etc.)

		~~Smart Card Handbook, pp. 263~~
CD		Ross Anderson and Markus Kuhn, "Tamper Resistance -- A Cautionary Note", The Second USENIX Workship on Electronic Commerce Proceedings, Oakland, California , Nov. 18-21, 1996, pp. 1-11
CD		Marc Joye, Arjen K. Lenstra and Jean-Jacques Quisquater, "Chinese Remaindering Based Cryptosystems in the Presence of Faults", to appear in Journal of Cryptology, pp. 1-5
CD		Peter Montgomery, "Modular Multiplication Without Trial Division", Mathematics of Computation, Volume 44, No. 170, April 1985, pp. 519-521.

EXAMINER [signature] DATE CONSIDERED 7/5/04

EXAMINER: Initial if citation is considered, whether or not citation is in conformance with MPEP 609; draw a line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant

PTO1449

BEST AVAILABLE COPY

OIPE JAN 0 8 2002 PATENT & TRADEMARK OFFICE

Form PTO 1449	Atty. Docket Number	Serial Number
U.S. Department of Commerce Patent and Trademark Office	Nitt-0028	~~To be assigned~~ 09/935654
Information Disclosure Statement by Applicant	Applicant KAMINAGA et al.	
	Filing Date Concurrently herewith	Group 2124

RECEIVED JAN 14 2002 Technology Center 2100

U.S. Patent Documents

Examiner Initial		Document Number	Date	Name	Class	Subc lass	Filing Date

Foreign Patent Documents

Examiner Initial		Document Number	Filing Date	Country	Clas s	Sub-class	Translation	
							Yes	No
CD		EP 0 801 345 A1	4/2/97	EPO			X	
CD		EP 1 006 492 A1	11/25/99	EPO			X	
CD		EP 1 134 653 A2	3/15/01	EPO			X	

Other Documents (Including Author, Title, Date Pertinent Pages, Etc.)

CD		Paul C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems, Advances in Cryptology - Crypto 96, 16th Annual International Cryptology Conference, Aug 18-22, 1996, Vol. Conf. 16, pp. 104-113.
CD		Thomas S. Messerges, Ezzy A. Dabbish, Robert H. Sloan, "Power Analysis Attacks of Modular Exponentiation on Smartcards", Cryptographic Hardware and Embedded Systems, International workshop August 1999, pp 144-157

RECEIVED JAN 14 2002 Technology Center 2100

Examiner	Date Considered
	7/5/04

Examiner: Initial if citation is considered, whether or not citation is in conformance with MPEP 609; draw a line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant

PTO1449

BEST AVAILABLE COPY